

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-345798

(43)Date of publication of application : 14.12.2001

(51)Int.Cl. H04L 9/08  
G06F 1/00  
G06F 12/00  
G06F 12/14  
G09C 1/00

(21)Application number : 2000-162036

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 31.05.2000

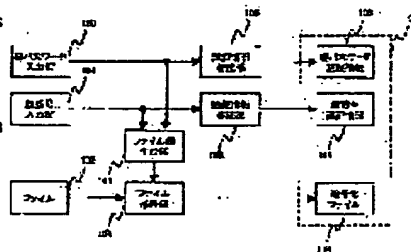
(72)Inventor : INAGAKI SATORU  
KOYAMA KAZUHIRO  
EMURA SATOSHI  
HIDAKA NORIYUKI  
MATSUZAKI NATSUME

## (54) APPARATUS FOR ENCRYPTING/DECRYPTING FILE

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To overcome the problem of a conventional apparatus for encrypting/decrypting a file using a password such that a password must be inputted every time when a file is encrypted or decrypted, and the problem of an conventional apparatus for encrypting/decrypting a file using a memory card that it is difficult to decrypt the file when the memory card is missed.

**SOLUTION:** A key password and a key number stored on a memory card are read in from a key password input section 100 and a key number input section 101. An encryption key is generated, based on them and a file is encrypted. An encrypted file can be decrypted by inserting the memory card storing the key password or the key number, or by inputting the key password and the key number.



## LEGAL STATUS

[Date of request for examination] 08.01.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than withdrawal the examiner's decision of rejection or application converted registration]

[Date of final disposal for application] 11.05.2005

[Patent number]

BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-345796

(P2001-345796A)

(43) 公開日 平成13年12月14日 (2001. 12. 14)

(51) Int.Cl. <sup>7</sup>	識別記号	P I	ページ(参考)
H 0 4 L 9/08		G 0 6 F 1/00	3 7 0 E 5 B 0 1 7
G 0 6 F 1/00	3 7 0	12/00	5 3 7 H 5 B 0 8 2
12/00	5 3 7	12/14	3 2 0 B 5 J 1 0 4
12/14	3 2 0		3 2 0 C
		G 0 9 C 1/00	6 3 0 Z

審査請求 未請求 請求項の数24 O L (全 15 頁) 最終頁に続く

(21) 出願番号 特願2000-162036(P2000-162036)

(22) 出願日 平成12年5月31日 (2000. 5. 31)

(71) 出願人 00005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 稲垣 悟

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72) 発明者 小山 和弘

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(74) 代理人 100097445

弁理士 岩橋 文雄 (外2名)

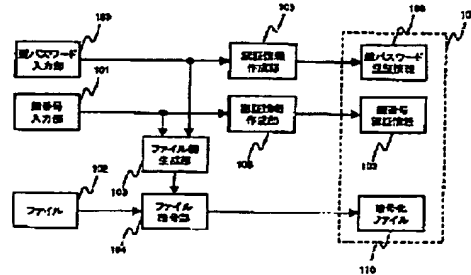
最終頁に続く

(54) 【発明の名称】 ファイル暗号復号装置

## [57] 【要約】

【課題】 従来、パスワードによる暗号復号装置においては、ファイルの暗号や復号処理を行うたびにパスワードを入力する必要があった。またメモリカード等を利用した暗号復号装置においては、メモリカードの紛失により、ファイルの復号が困難になるといった課題があった。

【解決手段】 鍵パスワード入力部100と鍵番号入力部101とから、メモリカード上に格納された鍵パスワードと鍵番号とが読み込まれる。これらに基づき暗号鍵が生成され、ファイルが暗号化される。復号時には、鍵パスワードもしくは暗号鍵が格納されたメモリカードを挿入するか、鍵パスワードと鍵番号とを入力することにより暗号ファイルを復号化することができる。



1

## 【特許請求の範囲】

【請求項1】 ファイルを入力するファイル入力手段と、

鍵パスワードを入力する鍵パスワード入力手段と、  
鍵生成情報を入力する鍵生成情報入力手段と、  
前記鍵パスワードと前記鍵生成情報とに基づきファイル鍵を生成するファイル鍵生成手段と、  
前記ファイルを前記ファイル鍵により暗号化し、暗号化ファイルを出力するファイル暗号手段とを備えたことを特徴とするファイル暗号装置。

【請求項2】 暗号化ファイルを入力とし、  
鍵パスワードを入力する鍵パスワード入力手段と、  
鍵生成情報を入力する鍵生成情報入力手段と、  
前記鍵パスワードと前記鍵生成情報とに基づき、ファイル鍵を生成するファイル鍵生成手段と、  
前記ファイル鍵により、前記暗号化ファイルを復号するファイル復号手段とを備えたことを特徴とするファイル復号装置。

【請求項3】 前記ファイル暗号手段は、前記鍵パスワードの認証情報を前記暗号化ファイルのヘッダに添付し、  
前記ファイル復号装置において、前記認証情報を用いて前記鍵パスワード入力手段から入力された鍵パスワードの認証を行う認証手段を備えたことを特徴とする請求項1または請求項2記載のファイル暗号復号装置。

【請求項4】 前記ファイル暗号手段は、前記鍵生成情報の認証情報を前記暗号化ファイルのヘッダに添付し、  
前記ファイル復号装置において、前記認証情報を用いて前記鍵生成情報入力手段から入力された鍵生成情報の認証を行う認証手段を備えたことを特徴とする請求項1または請求項2記載のファイル暗号復号装置。

【請求項5】 前記ファイル暗号手段は、前記鍵生成情報を前記暗号化ファイルのヘッダに添付し、  
前記ファイル復号装置における鍵生成情報入力手段は、前記暗号化ファイルのヘッダから鍵生成情報を抽出することを特徴とする請求項1または請求項2記載のファイル暗号復号装置。

【請求項6】 前記ファイル鍵生成情報は、所定の暗号鍵で暗号化されてヘッダに添付されることを特徴とする請求項5記載のファイル暗号復号装置。

【請求項7】 前記鍵パスワードを可搬媒体に格納し、  
前記鍵パスワード入力手段は、前記可搬媒体に格納された鍵パスワードを読み込むことを特徴とする請求項1または請求項2記載のファイル暗号復号装置。

【請求項8】 ユーザ名やユーザパスワード等のユーザ情報を入力するユーザ情報入力手段と、  
ユーザ情報と鍵パスワードとを関連付けて管理するユーザ管理手段と、  
ファイルを入力するファイル入力手段と、  
鍵生成情報を入力する鍵生成情報入力手段と、

(2)

特開2001-345796

2

前記ユーザ情報に基づき、前記ユーザ管理手段から鍵パスワードを抽出する鍵パスワード抽出手段と、  
前記鍵パスワードと前記鍵生成情報とに基づきファイル鍵を生成するファイル鍵生成手段と、  
前記ファイルを前記ファイル鍵により暗号化し、暗号化ファイルを出力するファイル暗号手段とを備えたことを特徴とするファイル暗号装置。

【請求項9】 暗号化ファイルを入力とし、  
ユーザ名やユーザパスワード等のユーザ情報を入力するユーザ情報入力手段と、

ユーザ情報と鍵パスワードとを関連付けて管理するユーザ管理手段と、  
鍵生成情報を入力する鍵生成情報入力手段と、  
前記ユーザ情報に基づき、前記ユーザ管理手段から鍵パスワードを抽出する鍵パスワード抽出手段と、  
前記鍵パスワードと前記鍵番号とに基づき、ファイル鍵を生成するファイル鍵生成手段と、  
前記ファイル鍵により、前記暗号化ファイルを復号するファイル復号手段とを備えたことを特徴とするファイル復号装置。

【請求項10】 前記ファイル暗号手段は、前記鍵生成情報の認証情報を前記暗号化ファイルのヘッダに添付し、

前記ファイル復号装置において、前記認証情報を用いて前記鍵生成情報入力手段から入力された鍵生成情報の認証を行う認証手段を備えたことを特徴とする請求項8または請求項9記載のファイル暗号復号装置。

【請求項11】 前記ファイル暗号手段は、前記鍵生成情報を前記暗号化ファイルのヘッダに添付し、

前記ファイル復号装置における鍵生成情報入力手段は、前記暗号化ファイルのヘッダから鍵生成情報を抽出することを特徴とする請求項8または請求項9記載のファイル暗号復号装置。

【請求項12】 前記ファイル鍵生成情報は、所定の暗号鍵で暗号化されてヘッダに添付されることを特徴とする請求項11記載のファイル暗号復号装置。

【請求項13】 前記ユーザ情報または鍵生成情報とを可搬媒体に格納し、前記ユーザ情報入力手段または鍵生成情報入力手段は、前記可搬媒体に格納されたユーザ情報または鍵生成情報を読み込むことを特徴とする請求項8または請求項9記載のファイル暗号復号装置。

【請求項14】 前記鍵パスワードを可搬媒体に格納し、前記ファイル鍵生成手段において、前記可搬媒体から鍵パスワードが入力されることを特徴とする請求項9記載のファイル復号装置。

【請求項15】 前記鍵生成情報は、鍵の種類を表す鍵番号であることを特徴とする請求項1または請求項2または請求項9または請求項10記載のファイル暗号復号装置。

50 【請求項16】 前記ファイル鍵生成手段は、前記鍵パ

(3) 特開2001-345796

3

スワードを第1の暗号化鍵に変換する鍵パスワード変換手段を備え、前記鍵番号をNとしたときに、前記第1の暗号化鍵に対して、所定の関数でN回変換を行い、ファイル鍵として出力することを特徴とする請求項15記載のファイル暗号復号装置。

【請求項17】 前記鍵生成情報は、暗号化ファイルの格納場所情報であることを特徴とする請求項1または請求項2または請求項8または請求項9記載のファイル暗号復号装置。

【請求項18】 前記ファイル暗号装置において、暗号化ファイルの格納場所を指定する格納場所指定手段を備え、前記格納場所指定手段で指定された格納場所情報が前記鍵生成情報入力手段から入力されることを特徴とする請求項17記載のファイル暗号復号装置。

【請求項19】 前記ファイル暗号装置において、暗号化ファイルの格納場所を検出する格納場所検出手段を備え、前記格納場所検出手段で検出された格納場所情報が、前記鍵生成情報入力手段から入力されることを特徴とする請求項17記載のファイル暗号復号装置。

【請求項20】 前記ファイル鍵生成手段は、前記鍵パスワードを第1の暗号化鍵に変換する鍵パスワード変換手段と、

前記格納場所情報を第2の暗号化鍵に変換する格納場所情報変換手段とを備え、

前記第1の暗号化鍵と前記第2の暗号化鍵とを所定の関数で変換し、ファイル鍵として出力することを特徴とする請求項17記載のファイル暗号復号装置。

【請求項21】 前記鍵生成情報は、装置のシリアル番号であることを特徴とする請求項1または請求項2または請求項8または請求項9記載のファイル暗号復号装置。

【請求項22】 装置のシリアル番号を抽出し、前記鍵生成情報入力手段に対してシリアル番号を送出するシリアル番号抽出手段を備えたことを特徴とする請求項21記載のファイル暗号復号装置。

【請求項23】 前記ファイル鍵生成手段は、前記鍵パスワードを第1の暗号化鍵に変換する鍵パスワード変換手段と、

前記シリアル番号を第2の暗号化鍵に変換するシリアル番号変換手段とを備え、

前記第1の暗号化鍵と前記第2の暗号化鍵とを所定の関数で変換し、ファイル鍵として出力することを特徴とする請求項21記載のファイル暗号復号装置。

【請求項24】 複数ユーザが使用する場合において、マスタユーザと一般ユーザとを規定し、

マスタユーザがマスタユーザの鍵パスワードに基づきマスタユーザ用の前記第1の暗号化鍵を生成し、

一般ユーザは一般ユーザの鍵パスワードと前記マスタユーザの鍵パスワードとに基づき一般ユーザ用の前記第1の暗号化鍵を生成することを特徴とする請求項16または

4

請求項20または請求項23記載のファイル暗号復号装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、計算機に付随した鍵情報を用いたファイルの暗号復号装置に関する。

【0002】

【従来の技術】従来のファイル暗号復号装置では、パスワードの入力もしくはICカードなどにより、ファイルの暗号および復号が行われていた。しかしながらパスワードによる方法では、ファイルの暗号・復号を行うたびにパスワードを要求されるためユーザに負担がかかるという問題点があった。またパスワードもしくはICカードによる方法でも、複数の暗号鍵を用いる場合に暗号鍵の管理が煩雑になるといった問題点があった。

【0003】この問題を解決するための従来のファイル暗号復号装置としては、例えば特開平9-204330号公報に記載されたものが知られている。このファイル暗号復号装置においては、ある暗号鍵を用いて暗号化されたファイルが、ディスク上の特定のフォルダ（先行文献では暗号フォルダと定義されているので、以下暗号フォルダという）に格納される。

【0004】暗号フォルダはあらかじめユーザにより作成され、認証用パスワードが設定される。これにより、暗号フォルダへのアクセス制御が行われる。また、暗号フォルダごとに暗号鍵生成用の任意数値が設定され、この数値と前記認証用パスワードとからファイル暗号用鍵が自動生成される。このファイル暗号用鍵によりファイルが暗号化され、暗号フォルダに格納される。

【0005】これにより、パスワードの入力なしに、ファイルの暗号化や復号化を行うことができる。

【0006】

【発明が解決しようとする課題】しかしながら従来の方法では、暗号フォルダに保存されている認証用パスワードファイルまたは暗号鍵生成用の任意数値を格納したファイルが、何らかの要因で破損した場合、暗号化されたファイルを復旧することは困難であるという課題がある。

【0007】本発明は、簡易な操作でファイルの暗号復号処理を行うことができ、かつ緊急時にはパスワードによるファイルの復号が可能であるファイル暗号復号装置を提供することを目的とする。

【0008】

【課題を解決するための手段】この課題を解決するために、請求項1記載の発明は、ファイルを入力するファイル入力手段と、鍵パスワードを入力する鍵パスワード入力手段と、鍵生成情報を入力する鍵生成情報入力手段と、前記鍵パスワードと前記鍵生成情報とに基づきファイル鍵を生成するファイル鍵生成手段と、前記ファイルを入力するファイル入力手段により暗号化し、暗号化ファイルを出

5

力するファイル暗号手段とを備えたものである。

【0009】また請求項2記載の発明は、暗号化ファイルを入力とし、鍵パスワードを入力する鍵パスワード入力手段と、鍵生成情報を入力する鍵生成情報入力手段と、前記鍵パスワードと前記鍵生成情報とに基づき、ファイル鍵を生成するファイル鍵生成手段と、前記ファイル鍵により、前記暗号化ファイルを復号するファイル復号手段とを備えたものである。

【0010】また請求項8記載の発明は、ユーザ名やユーザパスワード等のユーザ情報を入力するユーザ情報入力手段と、ユーザ情報と鍵パスワードとを関連付けて管理するユーザ管理手段と、ファイルを入力するファイル入力手段と、鍵生成情報を入力する鍵生成情報入力手段と、前記ユーザ情報に基づき、前記ユーザ管理手段から鍵パスワードを抽出する鍵パスワード抽出手段と、前記鍵パスワードと前記鍵生成情報とに基づきファイル鍵を生成するファイル鍵生成手段と、前記ファイル鍵を前記ファイル鍵により暗号化し、暗号化ファイルを出力するファイル暗号手段とを備えたものである。

【0011】また請求項9記載の発明は、暗号化ファイルを入力とし、ユーザ名やユーザパスワード等のユーザ情報を入力するユーザ情報入力手段と、ユーザ情報と鍵パスワードとを関連付けて管理するユーザ管理手段と、鍵生成情報を入力する鍵生成情報入力手段と、前記ユーザ情報に基づき、前記ユーザ管理手段から鍵パスワードを抽出する鍵パスワード抽出手段と、前記鍵パスワードと前記鍵番号とに基づき、ファイル鍵を生成するファイル鍵生成手段と、前記ファイル鍵により、前記暗号化ファイルを復号するファイル復号手段とを備えたものである。

【0012】また請求項14記載の発明は、前記鍵パスワードを可搬媒体に格納し、前記ファイル鍵生成手段において、前記可搬媒体から鍵パスワードが入力されることを特徴とするものである。

【0013】また請求項15記載の発明は、前記鍵生成情報が、鍵の種類を表す鍵番号であることを特徴とするものである。

【0014】また請求項16記載の発明は、前記ファイル鍵生成手段が、前記鍵パスワードを第1の暗号化鍵に変換する鍵パスワード変換手段を備え、前記鍵番号をNとしたときに、前記第1の暗号化鍵に対して、所定の関数でN回変換を行い、ファイル鍵として出力することを特徴とするものである。

【0015】また請求項17記載の発明は、前記鍵生成情報が、暗号化ファイルの格納場所情報であることを特徴とするものである。

【0016】また請求項21記載の発明は、前記鍵生成情報が、装置のシリアル番号であることを特徴とするものである。

【0017】また請求項24記載の発明は、複数ユーザ

(4)

特開2001-345796

6

が使用する場合において、マスタユーザと一般ユーザとを規定し、マスタユーザがマスタユーザの鍵パスワードに基づきマスタユーザ用の前記第1の暗号化鍵を生成し、一般ユーザは一般ユーザの鍵パスワードと前記マスタユーザの鍵パスワードとに基づき一般ユーザ用の前記第1の暗号鍵を生成することを特徴とするものである。

【0018】

【発明の実施の形態】以下、本発明の実施の形態について、図面を用いて説明する。

【0019】（実施の形態1）図1は本発明のファイル暗号復号装置におけるファイル暗号部の一実施例を示したものであり、100は鍵パスワードを入力する鍵パスワード入力部、101は鍵番号を入力する鍵番号入力部、102は暗号化したいファイル、103は前記鍵パスワードと前記鍵番号とからファイルを暗号化するためのファイル鍵を生成するファイル鍵生成部、104は前記ファイル鍵により前記ファイルを暗号化するファイル暗号部、105および106は前記鍵パスワードと前記鍵番号の認証情報を作成する認証情報作成部、107はヘッダも含めた暗号ファイル、108および109は鍵パスワードおよび鍵番号の認証情報、110は暗号化ファイルである。

【0020】図2は本発明のファイル暗号復号装置におけるファイル復号部の一実施例を示したものであり、図1と同じ符号のものは同じ機能を有するので詳細な説明は省略する。図2において、200は鍵パスワードを入力する鍵パスワード入力部、201は鍵番号を入力する鍵番号入力部、202は入力された鍵パスワードと鍵番号とを認証する認証部、203は鍵パスワードと鍵番号とからファイル鍵を生成するファイル鍵生成部、204はファイルを復号するファイル復号部、205は復号されたファイルである。

【0021】以上のように構成された本発明のファイル暗号復号装置について、以下その動作を述べる。

【0022】まずユーザが暗号化したいファイルの選択を行い、鍵パスワードの入力を行う。鍵パスワードはユーザが任意に設定することができる。単純な数文字程度のパスワードでもよいし、数十文字の長いパスワードでもよい。パスワードの入力は、通常あらかじめパスワードを格納しておいた記憶媒体から行われるものとする。本発明のファイル暗号復号装置にメモ리카ード等を挿入するスロットを備え、スロットに挿入されたメモ리카ードから鍵パスワードを読み込む仕組みを備えることで実現できる。もちろん、キーボード等の入力装置から鍵パスワードを入力してもよい。

【0023】鍵パスワードの入力が行われると、次に鍵番号が入力される。鍵番号は、例えば図3のようにファイルの使用目的毎に鍵を変えて暗号化するために用いられる。例えば鍵パスワードを、ある文字列もしくは数値列「A」は会社で使用するファイルと規定し、鍵番号

(5) 特開2001-345796

7

「1」は自分専用、鍵番号「2」はプロジェクト用、鍵番号「N」は連絡事項用のファイルを暗号化する際に用いる。これにより暗号化されたファイルを鍵番号で管理することができる。

【0024】鍵パスワードと鍵番号とが入力されるとファイル鍵生成部103でファイル暗号用の鍵であるファイル鍵が生成される。ファイル鍵は、例えばn文字以上の文字列をmビットの数値列に変換する関数と、mビットの数値列の並びを変えたmビットの数値列に変換する関数とを組み合わせて生成される。鍵生成の流れを図4に示す。図4においてS400はn文字以上の文字列をmビットの数値列に変換するステップであり、S401はmビットの数値列の並びを変える変換を行うステップである。鍵パスワードがn文字以上であればS400のステップへ入り、鍵パスワードがn文字以下の場合は所定のビットを追加してからS400のステップへ入る。次に鍵番号に応じてS401のステップが繰り返される。鍵番号が1であればS401の処理が一度だけ行われるが、鍵番号がNであれば、S401の処理がN回繰り返される。この結果ファイル鍵がmビットの数値列として出力される。

【0025】ファイル鍵生成部103でファイル鍵が生成されると、ファイル暗号部104でファイルが暗号化される。暗号化の方法はいかなるものでもよく、暗号アルゴリズムが必要とするファイル鍵のビット数に応じて、ファイル鍵生成部103で生成されるファイル鍵のビット数が決定される。

【0026】認証情報作成部105および106では、鍵パスワードおよび鍵番号のハッシュ値が鍵パスワード認証情報および鍵番号認証情報として出力される。暗号ファイル107には、ファイル暗号部104の出力である暗号化ファイルに、前記鍵パスワード認証情報108および鍵番号認証情報109がヘッダとして添付される。

【0027】次に復号処理について説明する。図2において、暗号ファイル107を入力とし、認証部202において鍵パスワード認証情報108および鍵番号認証情報109が抽出される。次にこのファイルを復号化するための鍵パスワードと鍵番号とを鍵パスワード入力部200および鍵番号入力部201から入力する。鍵パスワードは通常メモ리카ード等を挿入することで入力される

8

ドまたは鍵番号が正しくないと判断されれば、ファイル復号部204における復号処理は行われない。

【0028】なお、鍵パスワード入力部100および200において、メモ리카ードによる手段とキーボード等の入力手段のいずれでもよいとしたが、どちらか片方に制限してもよい。例えば鍵パスワードが意図して漏洩した場合には、メモ리카ードが挿入されている場合のみ暗号処理、復号処理を可能とすることにより、キーボードからパスワードを入力されることを防止できる。また、メモ리카ードを紛失した場合には、キーボード等の入力手段から入力される場合のみ暗号処理、復号処理を可能とすることにより、盗難されたメモ리카ードの悪用を防ぐことができる。この場合、メモ리카ード上には、所定の変換関数により変換した鍵パスワードを格納することにより、安全性を増すことができる。

【0029】また、鍵番号入力部101からは鍵の番号を入力するとして説明したが、任意の文字列を用いてもよい。この場合、任意の文字列を固定ビットの数値に変換する関数を設けて、図4におけるKの値を設定すればよい。例えば任意の文字列を8ビットの数値に変換した場合、Kの値は1から256のいずれかの値をとることになる。

【0030】（実施の形態2）図5は本発明のファイル暗号復号装置におけるファイル暗号部の一実施例を示したものであり、図1と同じ符号のものは同じ機能を有するので詳細な説明は省略する。図5において、500は鍵番号を暗号化する暗号処理部、501は鍵番号が暗号化された鍵番号情報である。

【0031】図6は本発明のファイル暗号復号装置におけるファイル復号部の一実施例を示したものであり、図1、図2、図5と同じ符号のものは同じ機能を有するので詳細な説明は省略する。図6において、600は暗号ファイル107のヘッダ部にある鍵パスワード認証情報を抽出し、鍵パスワード入力部200で入力された鍵パスワードの認証を行う認証部、601は鍵番号情報501の復号処理を行い、鍵番号を出力する復号処理部、602は鍵パスワードと鍵番号とからファイル鍵を生成するファイル鍵生成部である。

【0032】以上のように構成された本発明のファイル暗号復号装置について、以下その動作を述べる。

【0033】鍵パスワードが格納されたメモ리카ードを

BEST AVAILABLE COPY

(6) 特開2001-345796

9

ファイル107のヘッダ部に添付される。実施の形態1では、暗号ファイル107の中に鍵番号の認証情報をヘッダとして添付したのに対して、実施の形態2では、鍵番号そのものを暗号化してヘッダに添付する点で異なっている。

【0034】次に復号処理について説明する。ユーザがメモ리카ードを挿入すると、鍵パスワード入力部200においてメモ리카ード上の鍵パスワードが読み込まれる。認証部600では、入力された鍵パスワードと暗号ファイル107のヘッダに添付された鍵パスワード認証情報108とが比較される。復号処理部601では暗号ファイル107のヘッダに添付された鍵番号情報501（暗号化された鍵番号）から、所定の鍵で復号化して鍵番号を取り出す。認証部600において、入力された鍵パスワードが正しいと判断されれば、ファイル鍵生成部602においてファイル鍵が生成され、ファイル復号部204で復号処理が行われる。認証部600において入力された鍵パスワードが正しくないと判断された場合には、ファイル鍵生成部602で鍵が生成されず、ファイルの復号は行われない。この場合、正しいパスワードの入力を促すメッセージを表示しながら、鍵パスワード入力待ち状態を保つてもよい。

【0035】実施の形態1では、ファイルの復号時に、暗号ファイルに対してどの鍵を使用したのかを指定する必要があったが、実施の形態2ではファイル復号時に鍵番号の指定が必要である。

【0036】（実施の形態3）図7は本発明のファイル暗号復号装置におけるファイル暗号部の一実施例を示したものであり、図1と同じ符号のものは同じ機能を有するので詳細な説明は省略する。図7において、700は暗号ファイルの格納場所を指定する格納場所指定部、701は鍵パスワードと格納場所情報とからファイル鍵を生成するファイル鍵生成部、702は格納場所の認証情報を作成する認証情報作成部、703は格納場所の認証情報である。

【0037】図8は本発明のファイル暗号復号装置におけるファイル復号部の一実施例を示したものであり、図2および図6と同じ符号のものは同じ機能を有するので詳細な説明は省略する。図8において、800は暗号ファイルの格納場所を抽出する格納場所抽出部、801は格納場所抽出部で抽出された格納場所情報と、暗号ファイル内の格納場所認証情報703とを比較する認証部、802は鍵パスワードと格納場所情報とからファイル鍵を生成するファイル鍵生成部である。

【0038】以上のように構成された本発明のファイル暗号復号装置について、以下その動作を述べる。

【0039】まず暗号処理について述べる。図7において、格納場所指定部700では暗号化されたファイルの保存場所の指定を行う。指定方法は、直接フォルダ名を入力してもよいし、GUIなどによるマウスを用いた方

10

法でもよい。ここで格納場所指定部700の出力は、例えば暗号ファイルを格納するディレクトリの絶対パスの情報などである。暗号ファイルの格納場所が指定されると、ファイル鍵生成部701において、鍵パスワードと格納場所情報とに基づきファイル鍵が生成される。ファイル鍵は、例えば図9のような流れで生成される。鍵パスワードをn文字以上に変換した後、mビットの数値列に変換し、これをC1とする。（S900）次に格納場所情報をn文字以上に変換した後、mビットの数値列に変換し、これをC2とする。（S901）次にC1とC2との間で所定の演算を行い（S902）、ファイル鍵を生成する。

【0040】ファイル鍵が生成されると、ファイル暗号部104にてファイルが暗号化される。認証情報作成部105では鍵パスワードの認証情報が作成される。認証情報作成部702では、格納場所情報の認証情報が作成される。

【0041】実施の形態1および2では、鍵番号により使用する鍵を管理していたが、実施の形態3では、鍵の種類を変化させるために、暗号ファイルの格納場所の情報をを用いている。この様子を図10に示す。鍵番号で管理する場合は図3に示したように、鍵パスワードと鍵番号のテーブルにより管理が行われる。本実施の形態では、図10に示すように、ファイルの使用目的と格納フォルダ名とを関連付けることにより、ファイルの保存フォルダに基づき鍵管理を行うことができる。

【0042】次に復号処理について述べる。図8において、鍵パスワード入力部200から鍵パスワードが入力されると、認証部600において入力された鍵パスワードの認証が行われる。次に格納場所抽出部800において、暗号ファイル107の格納場所が抽出される。たとえば暗号ファイル107が保存されている絶対パスの情報などである。次に認証部801において、格納場所抽出部800で得られた格納場所情報の認証が行われる。

【0043】認証の結果、格納場所抽出部800で得られた格納場所と格納場所認証情報703とが一致した場合、すなわち復号時の格納場所が、暗号時の格納場所と同じ場合、格納場所情報がファイル鍵生成部802に入力される。認証部801での認証の結果、暗号時の格納場所と異なっている場合は、ファイル鍵生成部802には、認証に失敗したという情報が入力され、ファイル鍵は生成されない。

【0044】ここで、格納場所情報の認証に失敗した場合、ユーザがキーボード等の手段により格納場所情報を入力できるように設定してもよいし、認証に失敗した場合は復号不能という設定にしてもよい。認証に失敗した場合には復号不能とすれば、例えば他のディレクトリへ暗号ファイルをコピーすれば、復号不能となるので、ファイルコピーに対するセキュリティレベルを向上できるというメリットも生じる。

(7) 特開2001-345796

11

【0045】（実施の形態4）図11は本発明のファイル暗号復号装置におけるファイル暗号部の一実施例を示したものであり、図7と同じ符号のものは同じ機能を有するので詳細な説明は省略する。図11において、1100は格納場所指定部700で指定された格納場所情報を所定の暗号鍵で暗号化する暗号処理部、1101は暗号化された格納場所情報である。

【0046】図12は本発明のファイル暗号復号装置におけるファイル復号部の一実施例を示したものであり、図8と同じ符号のものは同じ機能を有するので詳細な説明は省略する。図12において、1200は暗号ファイル107のヘッダ部に添付された格納場所情報1101を所定の暗号鍵で復号化する復号処理部である。

【0047】以上のように構成された本発明のファイル暗号復号装置について、以下その動作を述べる。

【0048】まず、暗号処理について述べる。鍵パスワード入力部100において、例えばメモリカードから鍵パスワードが読み込まれる。次に格納場所指定部700から、暗号ファイルの格納場所が指定される。ファイル鍵生成部701において、入力された鍵パスワードと格納場所情報とから、ファイル鍵が生成され、ファイル暗号部104においてファイルが暗号化される。

【0049】次に認証情報作成部105においては、入力された鍵パスワードの認証情報（例えばハッシュ値等）が作成され、暗号ファイルのヘッダ部に添付される。暗号処理部1100では、格納場所指定部700で指定された暗号ファイルの格納場所情報が、所定の暗号鍵で暗号化され、暗号ファイル107のヘッダに添付される。

【0050】次に復号処理について述べる。鍵パスワード入力部200において、例えばメモリカードにより鍵パスワードが入力される。入力された鍵パスワードは、認証部600において、暗号ファイル107のヘッダに添付された鍵パスワード認証情報108と比較される。認証が正しく行われた場合、認証部600からは鍵パスワードが出力され、認証に失敗すれば、認証に失敗した旨の情報が出力される。復号処理部1200では、暗号ファイル107のヘッダ部に格納された格納場所情報1101が、所定の暗号鍵を用いて復号処理される。ファイル鍵生成部では、認証部600での認証結果に基づき、認証が正しく行われた場合のみファイル鍵が生成され、ファイルの復号処理が行われる。

【0051】実施の形態3では、暗号ファイルヘッダに格納場所の認証情報のみを格納することとしたが、本実施の形態では暗号ファイルヘッダに、格納場所情報を暗号化して格納した。これにより、暗号ファイルをコピー（登録商標）ディスク等の記憶媒体を經由して他のマシンへ移動した場合でも、ファイルの復号が可能である。

【0052】（実施の形態5）図13は本発明のファイル

12

ル暗号復号装置におけるファイル暗号部の一実施例を示したものであり、図1と同じ符号のものは同じ機能を有するので詳細な説明は省略する。図13において、1300は装置のシリアル番号を抽出するシリアル番号抽出部、1301は鍵パスワードとシリアル番号とからファイル鍵を生成するファイル鍵生成部、1302は前記シリアル番号の認証情報を作成する認証情報作成部、1303は、シリアル番号の認証情報である。

【0053】図14は本発明のファイル暗号復号装置におけるファイル復号部の一実施例を示したものであり、図12と同じ符号のものは同じ機能を有するので詳細な説明は省略する。図14において、1400は装置のシリアル番号を抽出するシリアル番号抽出部、1401は抽出されたシリアル番号の認証を行う認証部、1402はファイル鍵を生成するファイル鍵生成部である。

【0054】以上のように構成された本発明のファイル暗号復号装置について、以下その動作を述べる。

【0055】まず暗号処理について述べる。シリアル番号抽出部1300では、ファイル暗号復号装置に付されているシリアル番号が抽出される。ファイル鍵生成部1301では、鍵パスワード入力部100から入力された鍵パスワードと、シリアル番号抽出部1300で抽出されたシリアル番号とに基づきファイル鍵が生成される。ファイル鍵の生成は、例えば図9において「格納場所情報」の代わりに「シリアル番号」を用いることで説明できる。あるいはシリアル番号の長さをn文字に固定しておくことで、図15に示すように、鍵生成の流れを簡素化することもできる。ファイル鍵生成部1301において生成された鍵により、ファイルが暗号化される。認証情報作成部105では鍵パスワードの認証情報が作成され、認証情報作成部1302ではシリアル番号の認証情報が作成されて暗号ファイル107のヘッダに添付される。

【0056】次に復号処理について述べる。シリアル番号抽出部1400において、ファイル暗号復号装置のシリアル番号が抽出される。このシリアル番号は、認証部1401において、シリアル番号認証情報1303と照合される。認証に成功した場合、ファイル鍵生成部1402に対してシリアル番号が出力され、鍵パスワードとシリアル番号とに基づきファイル鍵が生成され、ファイルの復号が行われる。認証に失敗した場合は認証に失敗した旨の情報が出力され、ファイル鍵は生成されず、ファイルも復号されない。

【0057】実施の形態3において、認証に失敗した場合に復号不能とすれば、例えば他のディレクトリへ暗号ファイルをコピーすれば、復号不能となるので、ファイルコピーに対するセキュリティレベルを向上できるというメリットが生じた。本実施の形態では、装置のシリアル番号を判別するので、例えばフロッピーディスク等の可搬媒体や、ネットワーク経由で他のマシンへファイル



THIS PAGE BLANK (USPTO)

15

としたが、鍵番号を暗号化して暗号ファイルのヘッダに添付することもできる。この場合の暗号および復号処理を図20および図21に示す。図20において、図16と同じ符号のものは同じ機能を有する。図20において、2000は暗号処理部、2001は鍵番号情報である。暗号処理部2000では、鍵番号入力部1601から入力された鍵番号を所定の鍵で暗号化する。暗号化された鍵番号は、鍵番号情報2001として暗号ファイルのヘッダに添付される。

【0069】次に復号時の処理について説明する。図21において、2100は復号処理部である。復号処理部2100では、暗号ファイルに添付された鍵番号情報2001を所定の鍵で復号化し、鍵番号が取り出される。

【0070】このように、鍵番号が暗号ファイルのヘッダに添付されるので、鍵番号を入力することなく、復号ができる。

【0071】（実施の形態7）図22は本発明のファイル暗号復号装置におけるファイル暗号部の一実施例を示したものであり、図16と同じ符号のものは同じ機能を有するので詳細な説明は省略する。図22において、2200は暗号ファイルの格納場所を指定する格納場所指定部、2201は格納場所の認証情報を作成する認証情報作成部、2202は格納場所の認証情報である。

【0072】図23は本発明のファイル暗号復号装置におけるファイル復号部の一実施例を示したものであり、図16および図17と同じ符号のものは同じ機能を有するので詳細な説明は省略する。図23において、2300は暗号ファイルの格納場所を抽出する格納場所抽出部である。

【0073】まず暗号処理について説明する。格納場所指定部2200では、暗号ファイルを格納する場所の指定をユーザが行う。認証情報作成部2201で、格納場所の認証情報が作成され、格納場所認証情報2202として暗号ファイルのヘッダに添付される。

【0074】次に復号処理について説明する。格納場所抽出部2300において、暗号ファイルが格納されている場所の情報が抽出される。認証部1700で暗号ファイルに添付された格納場所認証情報と比較され、一致した場合はファイル復号処理が行われ、一致しない場合はファイルの復号処理は行われない。

【0075】このように構成することで、暗号ファイルのファイルコピーに対するセキュリティレベルを向上させることができる。

【0076】なお、上記説明では、格納場所の認証情報のみを暗号ファイルのヘッダに添付するとしたが、格納場所を所定の鍵で暗号化した情報をヘッダに添付してもよい。この場合を図24および図25を用いて説明する。図24は暗号処理を示しており、図22と同じ符号のものは同じ機能を有する。図24において2400は格納場所指定部の暗号処理を行う暗号処理部、2401

(9)

特開2001-345796

16

は暗号化された格納場所情報である。

【0077】図25は復号処理を示しており、図23および図24と同じ符号のものは同じ機能を有する。図25において、2500は格納場所情報2401を所定の鍵で復号する復号処理部である。

【0078】このように構成することで、鍵番号の入力の手間がかからず、暗号および復号処理を行うことができる。

【0079】また、実施の形態5で述べたように、装置のシリアル番号を暗号ファイルに添付してもよい。この様子を図26および図27を用いて説明する。

【0080】図26は暗号処理を示しており、図16と同じ符号のものは同じ機能を有する。図26において、2600はシリアル番号抽出部、2601は認証情報作成部、2602はシリアル番号の認証情報である。

【0081】図27は復号処理を示しており、図17および図26と同じ符号のものは同じ機能を有する。図27において、2700はシリアル番号抽出部、2701はシリアル番号の認証を行う認証部である。

【0082】シリアル番号抽出部2600において、装置のシリアル番号が抽出される。認証情報作成部2601にてシリアル番号の認証情報が作成されて暗号ファイル1608のヘッダ部に添付される。復号時には、シリアル番号抽出部2700で装置のシリアル番号が抽出され、認証部2701でファイルヘッダに添付されたシリアル番号認証情報2602と比較される。比較の結果一致すれば復号が行われ、一致しなければ復号は行われない。これにより、暗号時と異なる装置で復号することを防ぐことができる。

【0083】

【発明の効果】以上のように、請求項1および2記載の発明によると、通常の暗号復号処理時はメモリカードなどの記録媒体に格納された暗号鍵が用いられるが、暗号鍵が鍵パスワードから生成されているので、メモリカード紛失などの緊急時でも、鍵パスワードの入力により復号を行うことができる。

【0084】また請求項8および9記載の発明によると、ユーザ管理ファイルにより暗号鍵が管理されているので、通常にパソコンにログインする感覚でファイルの暗号復号処理を行うことができる。

【0085】また請求項14記載の発明によれば、メモリカード上に鍵パスワードを格納することにより、キーボード等から鍵パスワードを入力する手間を省くことができる。復号時にメモリカードを紛失した場合には、キーボード等から鍵パスワードを入力することでファイルの復号を行うことができる。また、この場合、メモリカードによるファイル復号を禁止することにより、紛失したメモリカードの悪用を防止することができる。

【0086】また請求項15記載の発明によれば、ファイルの使用目的に応じて鍵番号を設定できるので、複数

17

のファイルの管理が容易になる。

【0087】また請求項16記載の発明によれば、鍵パスワードから生成された暗号鍵に対して、同一の変換処理を繰り返して鍵を生成するので、簡単な処理で複数の暗号鍵を生成することができる。

【0088】また請求項17記載の発明によれば、鍵生成情報が、暗号ファイルの格納場所情報として与えられるので、鍵番号を覚えておく必要が無く、ファイルの格納場所と関連付けて鍵番号を管理できる。また他のディレクトリへ暗号ファイルをコピーした際に、復号を禁止できるので、ファイルのコピーに対するセキュリティレベルを向上することができる。

【0089】また請求項21記載の発明によれば、鍵生成情報が、装置のシリアル番号として与えられるので、フロッピーディスクやネットワーク経由で他の装置へファイルがコピーされた場合に復号を禁止することができる。

【0090】また請求項24記載の発明によれば、マスターユーザの暗号鍵に基づき一般ユーザの暗号鍵が生成されるので、一般ユーザが鍵パスワードを忘却した場合でも、マスターユーザが暗号鍵を生成することができる。またユーザ管理ファイルが何らかの要因で破損した場合でも、マスターユーザの鍵パスワードから一般ユーザの暗号鍵を生成することができる。

【図面の簡単な説明】

【図1】実施の形態1におけるファイル暗号処理のブロック図

【図2】実施の形態1におけるファイル復号処理のブロック図

【図3】鍵番号の説明図

【図4】鍵番号に基づく鍵生成のフロー図

【図5】実施の形態2におけるファイル暗号処理のブロック図

【図6】実施の形態2におけるファイル復号処理のブロック図

【図7】実施の形態3におけるファイル暗号処理のブロック図

【図8】実施の形態3におけるファイル復号処理のブロック図

【図9】格納場所情報に基づく鍵生成のフロー図

【図10】格納場所情報の説明図

【図11】実施の形態4におけるファイル暗号処理のブ

(10)

特開2001-345796

18

ロック図

【図12】実施の形態4におけるファイル復号処理のブロック図

【図13】実施の形態5におけるファイル暗号処理のブロック図

【図14】実施の形態5におけるファイル復号処理のブロック図

【図15】シリアル番号に基づく鍵生成のフロー図

【図16】実施の形態6におけるファイル暗号処理のブロック図

【図17】実施の形態6におけるファイル復号処理のブロック図

【図18】ユーザ管理ファイルの一例の説明図

【図19】ユーザ管理ファイルの他の例の説明図

【図20】実施の形態7における鍵番号に基づくファイル暗号処理のブロック図

【図21】実施の形態7における鍵番号に基づくファイル復号処理のブロック図

【図22】実施の形態7におけるファイル暗号処理のブロック図

【図23】実施の形態7におけるファイル復号処理のブロック図

【図24】実施の形態7における格納場所に基づくファイル暗号処理のブロック図

【図25】実施の形態7における格納場所に基づくファイル復号処理のブロック図

【図26】実施の形態7におけるシリアル番号に基づくファイル暗号処理のブロック図

【図27】実施の形態7におけるシリアル番号に基づくファイル復号処理のブロック図

【符号の説明】

100 鍵パスワード入力部

101 鍵番号入力部

102 ファイル

103 ファイル鍵生成部

104 ファイル暗号部

105 認証情報作成部

106 認証情報作成部

107 暗号ファイル

40 108 鍵パスワード認証情報

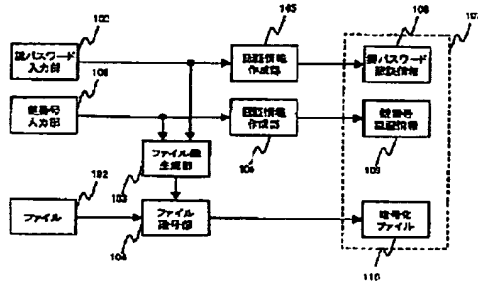
109 鍵番号認証情報

110 暗号化ファイル

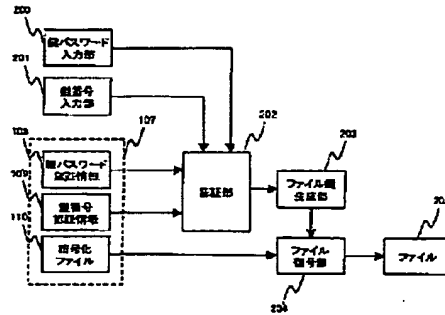
(11)

特開2001-345796

【図1】



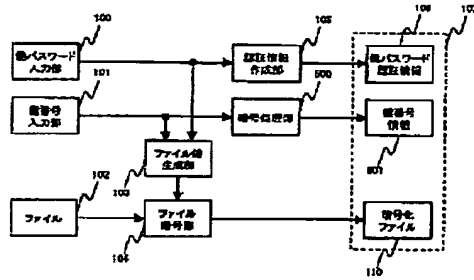
【図2】



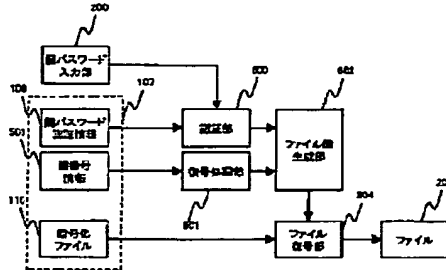
【図3】

パスワード	A	B	-----	N
目的	会社用	家庭用	-----	友人用
番号	1	自分のみ	自分のみ	自分のみ
	2	プロジェクト用	会社用	ごく親しい友人用
	...	...	...	...
	N	連絡事項用	全員用	友人一般用

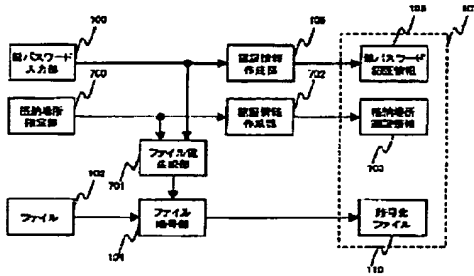
【図5】



【図6】



【図7】



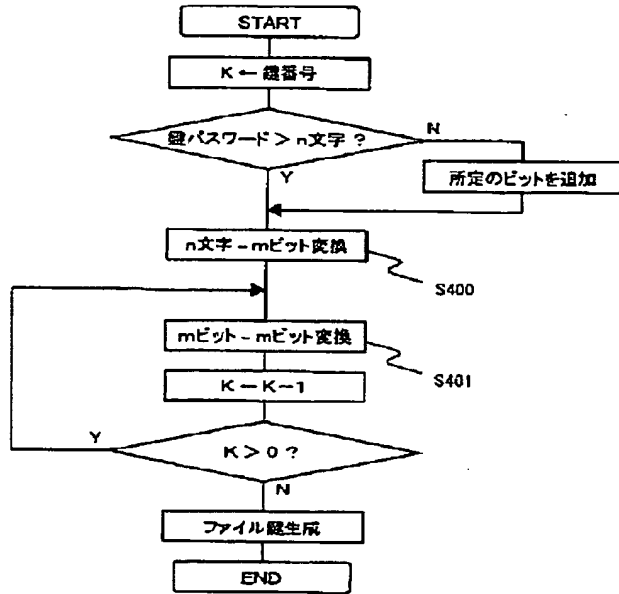
【図18】

ユーザ	パスワード	パスワード
ユーザA	H(DCA)	K(A)
ユーザB	H(DBS)	K(B)
...	...	...
ユーザN	H(DND)	K(D)

(12)

特開2001-345796

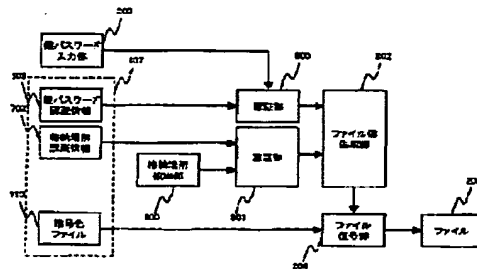
【図4】



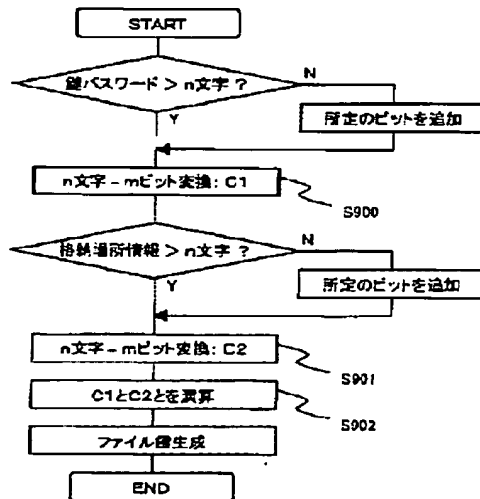
【図19】

ユーザ名	パスワード 暗号化情報	鍵パスワード
スーパーユーザ	H(P(S))	K(S)
ユーザA	H(P(A))	F(K(S), A)
ユーザB	H(P(B))	F(K(S), B)
...	...	...
ユーザN	H(P(N))	F(K(S), N)

【図8】



【図9】



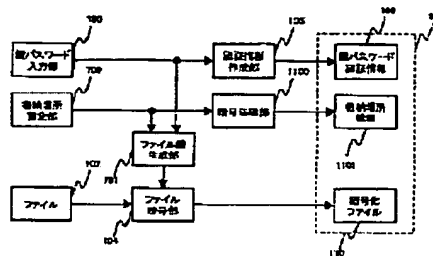
(13)

特開 2001-345796

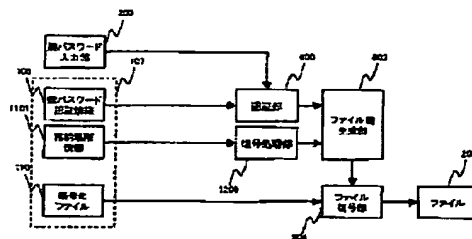
【圖10】

種別/キーワード	A	B	C	D
大分類	会社員	役員等	.....	法人内
内勤と フィールド	自分から	自分から	.....	自分から
	customer代表役員	customer代表役員	.....	customer代表役員
	プロジェクト用	販路用	.....	customer代表役員
	customer代表役員	customer代表役員	.....	customer代表役員
	.....	.....	.....	.....
	近隣関係者	会社員	.....	法人一般用
	customer代表役員	customer代表役員	.....	customer代表役員

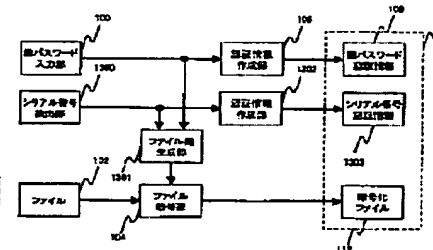
【图 1 1】



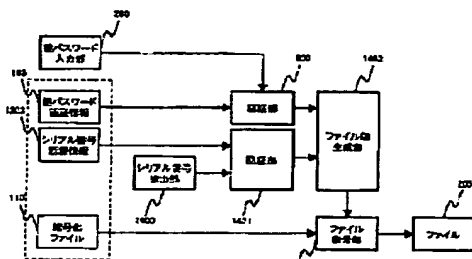
【圖 12】



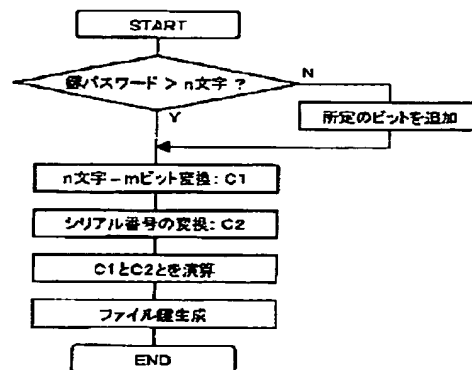
【圖 13】



【圖 14】



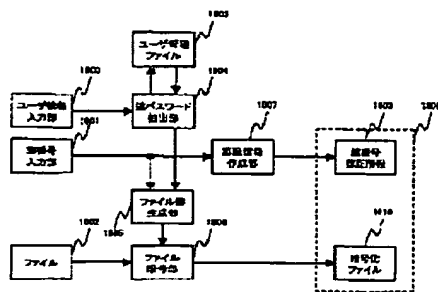
【圖 15】



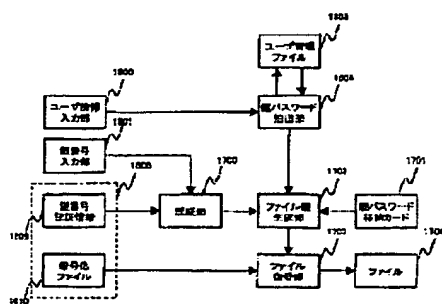
(14)

特開2001-345796

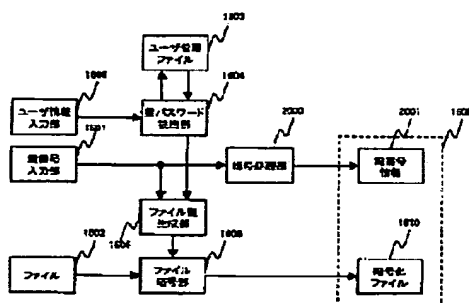
【~~8~~ 1 6】



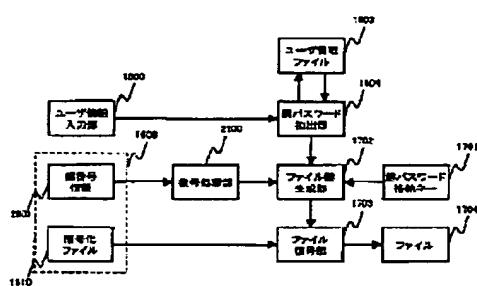
【圖 17】



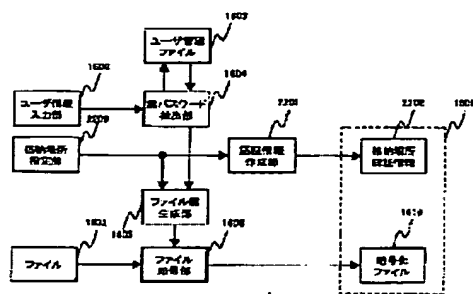
【圖 20】



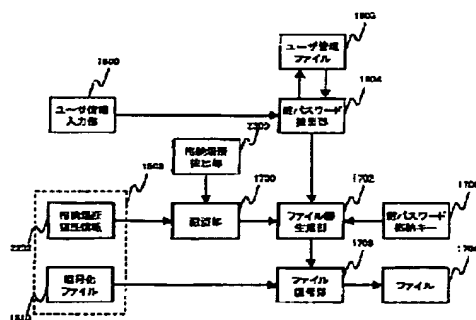
【例 2 1】



【圖 22】



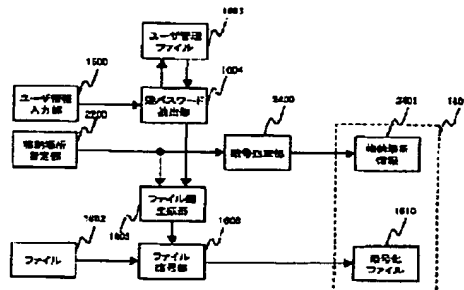
【图 23】



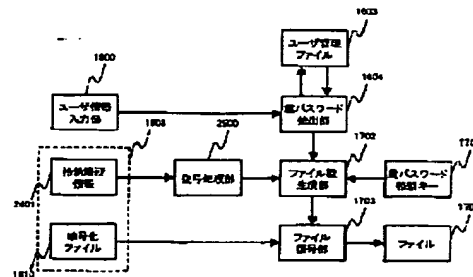
(15)

特開2001-345796

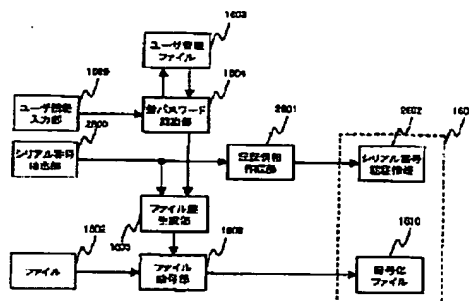
【图 2-4】



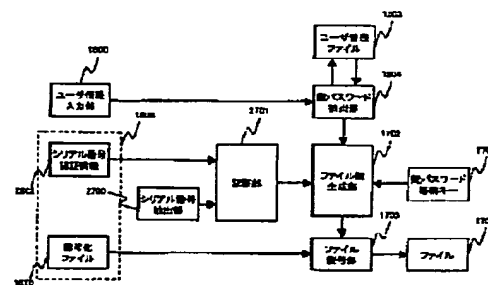
【圖 25】



【圖 26】



【圖 27】



フロントページの続き

(51) Int. Cl. ?

G O 9 C 1/00

識別記号

630

F I

H04L 9/00

テ-マ-ト' (参考)

601Z

(72) 发明者 江村 里志

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72) 発明者 日高 紀幸

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72) 発明者 松崎 なつめ

大坂府門真市大字門真1006番地 松下電器  
産業株式会社内

Fターム(参考) 5B017 AA03 BA05 BA07 CA16

5B082 EA12 GA02 GA11

5J104 AA01 AA07 AA16 EA04 EA06

EA11 EA26 KA01 NA01 NA05

NA35 NA38 PA14